REMARKS

Reconsideration and allowance of the subject application are requested.

Claims 1-18 are pending.

Claims 1-5 stand rejected under 35 U.S.C. §103 as being unpatentable over Reeds in view of Laufer. Applicants respectfully traverse this art grounds of rejection.

As the Examiner correctly notes, Reeds does not disclose or suggest "the iteration of the CMEA process employing an enhanced tbox function using an involutary lookup, the inputs to the enhanced tbox function being subjected to a permutation using one or more of the secret offsets to produce a permutation result," as recited in claim 1.

With respect to using an involuntary lookup, the Examiner relies upon Laufer as teaching an involution function. The Examiner contends that one skilled in the art would have been motivated to combine the teachings of Reeds using the involutions of Laufer with the table lookup "because use of lookup is less resource intensive which is exactly what is needed for cellular phones, which have limited resources." See page 5 of the April 6, 2004 Office Action.

Applicants respectfully submit that the Examiner has fallen victim to the hindsight syndrome and used Applicants' own teachings against them. Laufer is a textbook and provides absolutely no motivation regarding the field of use for involution functions or the advantages thereof. Accordingly, Laufer provides no motivation for the application of the involution function as set forth by the Examiner. Additionally, Reeds does not recognize, as the Examiner has already noted, any benefits or motivation for using an involution function or table lookup. Instead, the Examiner has manufactured a motivation regarding the use of an involution function in an involuntary lookup for use in a system in Reeds. The Examiner's constructed motivation is that involution with table lookup would be less resource intensive. If less resource intensive, if the Examiner means that less memory would be required of the cell phone, then the Examiner is clearly wrong as the use of a table lookup for the involution would greatly increase the amount of memory required of the cell phone. The Examiner has shown absolutely no motivation as to why one skilled in the art would be motivated to increase the memory of the cell phone and therefore the cost of the cell phone (a highly priced competitive market), and how this is less resource intensive. Applicants respectfully submit that the Examiner, in an attempt to reject claim 1, has pieced together teachings from different references without a true motivation therefore, but instead under an unsupported motivation, while under the effects of the hindsight syndrome. Applicants respectfully request that the Examiner reconsider this rejection.

With regard to the inputs of the enhanced tbox function being subjected to a permutation using one or more secret offsets, the Examiner states "it is well-known in the art that permutations are used to eliminated the characteristic footprint of the encryption algorithm. DES using permutations with the iterative encryption algorithm together with the key scheduling. For this reason one of ordinary skill in the art at the time the invention was made would have been motivated to incorporate permutations because they help remove the characteristic signature (footprint) of the algorithm and thus making it more difficult for a cryptanalysis to find an entrance into the cipher." See page 4 of the April 6, 2004 Office Action.

Again it appears that the Examiner has fallen victim to the hindsight syndrome. Neither Reeds, as admitted by the Examiner, nor Laufer, teach subjecting the inputs to an enhanced tbox function to a permutation using one or more secret offsets. The Examiner made some obscure reference to DES and the use thereof in an encryption algorithm, but does not provide any teaching in any reference that shows that the inputs to an enhanced tbox function are being permutated using one or more secret offsets. Instead, the Examiner takes a form of official notice that this would be well known to one skilled in the art. Applicants therefore challenge the Examiner to produce a reference to supply this teaching, and further challenge the Examiner to find motivation as to why one skilled in the art would have permutated the inputs to an enhanced tbox function using one or more secret offsets.

Applicants entirely expect that the Examiner will be unable to find these teachings, and submit that the Examiner's hindsight syndrome has led him down this erroneous path. Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the art grounds of rejection.

In subsequent art grounds of rejection the Examiner also cites the teachings in Vernam, G. S., "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," Journal A.I.E.E. Vol. XVI, pgs 109-115, Dec. 1926, and Takaragi et al. (U.S. Patent No. 5,222,139) in combination with Reeds in view Laufer in rejecting claim 6-7 and 7-18. However, none of these additionally cited references overcome the disclosure and suggested deficiencies discussed above with respect to claim 1. Consequently, claim 1 is patentable over the art cited by the Examiner. The remaining claims, alone or by their dependency upon claim 1, recite similar limitations to those discussed above with respect to claim 1, and are patentable at least for the reasons stated above with respect to claim 1.

CONCLUSION

In view of above remarks, reconsideration of the outstanding rejection and allowance of the pending claims is respectfully requested.

In the event that any outstanding matters remain in this application, Applicant requests that the Examiner contact the undersigned at the telephone number listed below.

Pursuant to 37 C.F.R. 1.17 and 1.136(a), the Applicants respectfully petition for a two (2) month extension of time for filing a response in connection with the present application, and the required fee of $420.00 is attached.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY & PIERCE, P.L.C.

By____________________________
Gary D. Yacura
Reg. No. 35,416

GDY:jcp

P.O. Box 8910
Reston, VA 20195
(703) 668-8000